CLAIMS

1. A method comprising:

decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting, under the influence of the cryptographic processor, the resultant data; and

writing the encrypted resultant data to a memory surface associated with the video card;

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

2. The method of claim 1, wherein the memory surfaces reside on the video card.

3. The method of claim 1, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

4. The method of claim 1, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

5. The method of claim 1, wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis.

6. The method of claim 1, wherein the cryptographic processor comprises a hardware component mounted on the video card.

7. The method of claim 1, wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card.

8. The method of claim 1, wherein the cryptographic processor comprises a trusted component.

9. The method of claim 1 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

10. The method of claim 1 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

11. The method of claim 1, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

12. A method comprising:

decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting, under the influence of the cryptographic processor, the resultant data; and

writing the encrypted resultant data to a memory surface associated with the video card;

said acts of decrypting and re-encrypting taking place on a per cache page basis.

13. The method of claim 12, wherein the memory surfaces reside on the video card.

14. The method of claim 12, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

15. The method of claim 12, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

16. The method of claim 12, wherein the act of decrypting and re-encrypting take place on a pixel-by-pixel basis.

17. The method of claim 12, wherein the cryptographic processor comprises a hardware component mounted on the video card.

18. The method of claim 12, wherein the cryptographic processor comprises an integrated circuit chip mounted on the video card.

19. The method of claim 12, wherein the cryptographic processor comprises a trusted component.

20. The method of claim 12 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

21. The method of claim 12 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

22. The method of claim 12, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

23. A method comprising:

decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to a video card memory surface associated with the video card,

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

24. The method of claim 23, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

25. The method of claim 23, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

26. The method of claim 23, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

27. The method of claim 23, wherein the acts of decrypting are performed using at least one key that was received from a trusted software component.

28. The method of claim 23 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

29. The method of claim 23 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

30. The method of claim 23, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

31. A method comprising:

decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to a video card memory surface associated with the video card,

said acts of decrypting and re-encrypting taking place on a per cache page basis.

32. The method of claim 31, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

33. The method of claim 31, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

34. The method of claim 31, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

35. The method of claim 31, wherein the acts of decrypting are performed using at least one key that was received from a trusted software component.

36. The method of claim 31 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the one or more memory surfaces.

37. The method of claim 31 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the one or more memory surfaces.

38. The method of claim 31, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

39. A system comprising:

means for decrypting, on a per cache page basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;

means for performing an operation on the decrypted data to provide resultant data;

means for re-encrypting, on a per cache page basis, the resultant data; and

means for writing the encrypted resultant data to a video card memory surface associated with the video card.

40. The system of claim 39, wherein the means for decrypting comprises, at least in part, cryptographic hardware inside the GPU.

41. The system of claim 39, wherein the means for performing comprises a GPU.

42. The system of claim 39, wherein the means for re-encrypting comprises, at least in part, cryptographic processor hardware mounted on the video card.

43. The system of claim 39, wherein said means for decrypting and re-encrypting comprise one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

44. The system of claim 39 further comprising means for pooling decrypted pages to avoid multiple decryptions of a page that might be needed more than once.

45. A system comprising:

a video card;

a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device;

memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card and configured to control encryption and decryption on the video card, the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted, on a per cache page basis, in connection with an operation that is to be performed on the data by the GPU; and

the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis, to an output memory surface.

46. The system of claim 45, wherein the cryptographic processor is configured to use block ciphers to effect encryption and decryption.

47. The system of claim 45, wherein the cryptographic processor is configured to use one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

48. The system of claim 45, wherein the cryptographic processor comprises a hardware component mounted on the video card.

49. The system of claim 45, wherein the cryptographic processor comprises an integrated circuit chip.

50. The system of claim 45, wherein the cryptographic processor comprises a trusted component.

51. The system of claim 45, wherein the cryptographic processor is configured to set up a session key with a trusted software component.

52. A computer system embodying the system of claim 45.

53. A method comprising:

providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;

associating, with each input memory surface, a decryptor that is uniquely able to decrypt the encrypted data that is held by the associated input memory surface;

decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to an output memory surface associated with the video card,

at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.

54. The method of claim 53, wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card.

55. The method of claim 53, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data.

56. The method of claim 53, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data, and wherein negotiated key indices are used to identify and regulate which keys are used in decrypt and re-encrypt operations.

57. The method of claim 53, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

58. The method of claim 53, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

59. The method of claim 53, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

60. The method of claim 53, wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card.

61. The method of claim 60, wherein the cryptographic processor comprises an integrated circuit chip.

62. The method of claim 60, wherein the cryptographic processor comprises a trusted component.

63. The method of claim 53, wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface.

64. The method of claim 53 further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available.

65. The method of claim 53 further comprising decrypting the encrypted resultant data for rendering on a display device.

66. The method of claim 53 further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device.

67. The method of claim 53 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces.

68. The method of claim 53 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces.

69. The method of claim 53, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

70. A method comprising:

providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;

associating, with each input memory surface, a decryptor that is uniquely able to decrypt the encrypted data that is held by the associated input memory surface;

decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;

performing an operation on the decrypted data using the GPU to provide resultant data;

re-encrypting the resultant data; and

writing the encrypted resultant data to an output memory surface associated with the video card,

said acts of decrypting and re-encrypting taking place on a per cache page basis.

71. The method of claim 70, wherein the act of providing the multiple input memory surfaces comprises providing at least one input memory surface on the video card.

72. The method of claim 70, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data.

73. The method of claim 70, wherein the act of re-encrypting comprises using an encryptor that is uniquely associated with the output memory surface to re-encrypt the resultant data, and wherein negotiated key indices are used to identify and regulate which keys are used in decrypt and re-encrypt operations.

74. The method of claim 70, wherein the acts of decrypting and re-encrypting are performed using one or more block ciphers.

75. The method of claim 70, wherein the acts of decrypting and re-encrypting are performed, at least in part, using one or more block ciphers whose block size bears an integer size relation to a cache line of a cache page.

76. The method of claim 70, wherein the acts of decrypting and re-encrypting take place on a pixel-by-pixel basis.

77. The method of claim 70, wherein the acts of decrypting and re-encrypting are performed under the influence of a cryptographic processor that resides on the video card.

78. The method of claim 77, wherein the cryptographic processor comprises an integrated circuit chip.

79. The method of claim 77, wherein the cryptographic processor comprises a trusted component.

80. The method of claim 70, wherein the act of decrypting is performed only when the GPU is to perform an operation on data that resides on a particular input memory surface.

81. The method of claim 70 further comprising restricting one or more operations that can be performed by the GPU based on whether encrypted output is available.

82. The method of claim 70 further comprising decrypting the encrypted resultant data for rendering on a display device.

83. The method of claim 70 further comprising decrypting, with a display convertor, the encrypted resultant data for rendering on a display device.

84. The method of claim 70 further comprising receiving pre-swizzled encrypted data and writing the pre-swizzled encrypted data to the input memory surfaces.

85. The method of claim 70 further comprising receiving pre-swizzled encrypted data that has been pre-swizzled by trusted software, and writing the pre-swizzled encrypted data to the input memory surfaces.

86. The method of claim 70, wherein the act of decrypting comprises caching decrypted pages in a local page pool cache to avoid multiple decryptions if a same page is needed.

87. A system comprising:

a video card;

a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device;

memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;

a cryptographic processor on the video card and configured to control encryption and decryption on the video card, the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card;

each individual input memory surface having its own unique associated key for decrypting encrypted data held thereon;

the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted on a per cache page basis so that the decrypted data can be operated upon by the GPU;

the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted on a per cache page basis to an output memory surface.

88. The system of claim 87, wherein the cryptographic processor is configured to control encryption and decryption using block ciphers.

89. The system of claim 87, wherein encryption and decryption takes place on a pixel-by-pixel basis.

90. The system of claim 87, wherein encrypted data held on an input memory surface is decrypted only when it is to be operated upon by the GPU.

91. The system of claim 87, wherein the cryptographic processor comprises an integrated circuit chip.

92. The system of claim 87, wherein the cryptographic processor comprises a trusted component.

93. The system of claim 87, wherein the cryptographic processor is configured to set up a session key with a trusted software component.

94. A computer system embodying the system of claim 87.